security baseline
PROTECTION | COMPLIANCE | RISK MANAGEMENT

Serviceomschrijving

tcas

Wat is de TCA Security Baseline?

In een wereld waarin cyberdreigingen zich constant ontwikkelen* is de Security Baseline een onmisbare schakel in uw informatie-beveiliging. Het is een volledig beheerde beveiligingsoplossing die uw beveiligingsmaatregelen controleert, rapporteert en waar nodig corrigeert, terwijl gebruikers flexibel en veilig kunnen blijven werken.

Gebaseerd op Microsoft 365-technologie, biedt deze baseline een gestandaardiseerde, schaalbare en toekomstbestendige aanpak voor informatiebeveiliging.

Transparant en schaalbaar

- Heldere licentiemodellen.
- Geen verrassingen in kosten of functionaliteit.
- Geen maandelijkse fee voor onderhoud en support.
- Eenvoudig beheer via 1 centraal portaal
- Snel op- en afschalen van gebruikers en apparaten.

Waarom heeft u de TCA Security Baseline nodig?

Wij handhaven strenge beveiligingsstandaarden en instellingen op de volgende kernonderdelen:

Toegang tot bedrijfsdata alleen vanuit geografisch specifieke gebieden of via beheerde apparaten.

Blokkade van verouderde protocollen (POP3, IMAP).

Multi-Factor Authenticatie (MFA) voor alle accounts.

Beveiliging van bedrijfsdata op privéapparaten via MAM (Microsoft App Protection)

Bescherming tegen misconfiguraties en foutieve handelingen.

Voor wie is de TCA Security Baseline?

De TCA Security Baseline is ideaal voor organisaties die:

- Willen voldoen aan de modernste beveiligingsnormen.
- Flexibel willen werken, zonder concessies aan veiligheid.
- Zelf controle willen houden over gebruikersbeheer.
- Voor organisaties die het maximale willen halen uit het Microsoft Ecosysteem

Optimale gebruikerservaring op elk apparaat

- Bedrijfseigen apparaten: Volledig beheerd, compliant en altijd toegang tot apps en data.
- Privéapparaten: Veilige toegang via browser, met isolatie van bedrijfsdata en bescherming tegen datalekken.
- Gebruik e-mail veilig op al uw apparaten, ook uw privé apparaten

Selfservice wordt veiliger én krachtiger

IT-afdelingen houden de regie, zonder de dagelijkse operatie te vertragen.

Selfservice blijft volledig beschikbaar: beheerders kunnen zelf accounts aanmaken, rechten toekennen, data delen en/of apparaten wissen/blokkeren.

Dankzij de onderliggende beveiligingslagen kunnen beheerders dit doen zonder risico op datalekken of misconfiguraties.

Het on-en offboarden van nieuwe medewerkers laat je met een gerust hart over aan je HR-afdeling.

Klaar voor compliance en audits

- Biedt templates om te voldoen aan eisen van o.a. NIS2, BIO en ISO27001.
- Automatische logging en rapportage van beveiligingsmaatregelen en afwijkingen.
- Beveiliging is geen losse laag, maar een integraal onderdeel van uw IT-structuur.

Veelgestelde vragen

Waarom is de implementatie van Security Baseline juist nu belangrijk?
Cyberdreigingen veranderen sneller dan ooit door technologie als AI. Voorkomen is beter dan genezen.

Zijn er maandelijkse abonnementskosten mee gemoeid?
De Security Baseline valt binnen het standaard dienstenportfolio

Welke beveiligingsmaatregelen zijn inbegrepen?
MFA, protocolblokkades, apparaatbeheer, geografische toegangscontrole, 24/7 monitoring en meer.

Is de Security Baseline geschikt voor mijn organisatie?
Ja, als je maximale veiligheid, flexibiliteit en zelf in controle blijven belangrijk vindt.

Helpt dit bij compliance en audits?
Ja, met templates, logging en rapportages voor o.a. NIS2, BIO, ISO27001.vz z z zz tttv

*Cybersecurity trends waarop Security Baseline inspeelt.

De belangrijkste maatregelen op een rijtje:

Maatregelen	Baseline	Informatie
Beveiliging van Apps op mobiele apparaten met app protectie	✓	Voor telefoon en tablet
Kopieren van data uit zakelijke apps naar privé apps blokkeren	Optie	Bijvoorbeeld het kunnen kopieren van tekst uit een zakelijke email naar Whatsapp
Blokkeren van bedrijfsapps backuppen naar een externe backupdienst	✓	Bijvoorbeeld naar iCloud of Google Cloud
Alle bedrijfsapps op mobiele apparaten elke 30 minuten deblokkeren met pincode/ faceID / vingerafdruk	✓	
Bedrijfsdata wordt geëncrypt binnen de bedrijfsapps	✓	Data wordt standaard versleuteld
Minimale versie OS (nog door fabrikant ondersteund)	✓	Oude (niet gesupporte) versies van IOS of Android worden niet meer ondersteund. We volgen hierbij de fabrikant
Na 10x foutieve inlog wordt de bedrijfsdata van het apparaat gewist	✓	Na 10 keer foutief ingeven van een wachtwoord worden alle gegevens van de telefoon of tablet verwijderd. Uiteraard niet van de server
Bedrijfsdata wordt gewist na deactivatie account	✓	Wanneer een account wordt geblokkeerd, bij bijvoorbeeld vertrek van een medewerker, dan worden alle bedrijfsdata gewist.
Inlog frequentie van 12 uur voor applicaties op niet compliant (vertrouwde) apparaten	✓	Elke 12 uur moet er opnieuw worden ingelogd met username, wachtwood en token
Inlog frequentie voor browser op niet compliant (vertrouwde) apparaten	✓	Bij gebruik van browsers op niet bedrijfsapparatuur, bijvoorbeeld een thuis pc/ internet café
Toestaan van locaties op niet beheerde computers, telefoons en tablets	✓	West Europa is standaard. Zuid-Europa en Noord-Europa kunnen optioneel worden toegevoegd.
Toestaan van locaties op beheerde computers, telefoons en tablets	✓	Overal toegang. Specifieke uitzonderingen (Rusland, China) daargelaten
MFA uitzondering op specifieke diensten	✓	Sommige specifieke diensten geven problemen met MFA. Deze worden uitgesloten
Blokkeren oude aanmeldprotocollen	✓	Alle verouderde aanmeld protocollen staan uit. Het is niet mogelijk om hiermee in te loggen of email op te halen.
MFA altijd aan	✓	
MFA whitelisting (uitzonderingen)	✗	Alleen in specifieke gevallen
Automatisch blokkeren bij risicovolle inlogpogingen	✓	
Verwijderen van mail met malafide inhoud	✓	Na ontvangst worden mails met malafide inhoud tussen de 1 en 4 uur verwijderd
Proactief verwijderen van mail met malafide inhoud	Optie	
Configureren van automatische regels om actief malafide situaties tegen tegaan	Optie	
Patchmanagement - (security)updates op Windows 11 en Igel apparaten	✓	
Patchmanagement - (security)updates op (Azure) servers	✓	
Secure Back-up: centraal-decentraal en geografisch gescheiden. Bij default altijd AAN	✓	
Antivirus & antimalware op Windows 11 apparaten	✓	
Antivirus & antimalware op IOS & Android apparaten	Optie	
Antivirus & antimalware op op (Azure) servers	✓	
Netwerk segemantatie. Scheiden van publieke en bedrijfsmatige netwerktoepassingen	✓	
Beveiligd wifi	✓	